IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:)
)
Christopher G. Steel)
)
Serial No.: 10/535,327) Group Art Unit: 2617
)
Filed: February 6, 2006) Examiner: Amancio Gonzalez
)
METHOD OF DISTRIBUTING) **Board of Patent Appeals and**
For: THE LOCATION DATA OF) **Interferences**
A MOBILE DEVICE)
)

Mail Stop: Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

In support of the notice of appeal filed on August 11, 2008, and pursuant to 37 C.F.R. § 41.37, Appellant presents this Appeal Brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 1-4 in the Final Office Action dated February 22, 2008, as clarified in the Advisory Action dated June 12, 2008. The appealed claims are set forth in the attached Claims Appendix.

1. Real Party in Interest

This application is assigned to Koninklijke Philips Electronics, N.V., the real party in interest.

2. Related Appeals and Interferences

There are no other appeals or interferences which would directly affect, be directly affected, or have a bearing on the instant appeal.

3. Status of the Claims

Claims 1-4 have been rejected in the Final Office Action. The final rejection of claims 1-4 is being appealed.

4. Status of Amendments

No amendments have been submitted by Appellant.

5. Summary of Claimed Subject Matter

The present invention, as recited in independent claim 1, relates to a method of distributing the location of a mobile device. The method comprises determining the location of the mobile device (MS2). (See Specification, p. 3, ll. 13-20; Figs. 1-2.) The determined location is encrypted using an encryption key. (See id., p. 4, ll. 4-8.) The encrypted location is transmitted to a server (IS). (See id., p. 3, ll. 26-30; Figs. 1, 3.) The encrypted location is stored at the server (IS). (See id., p. 4, ll. 4-8; Figs. 1, 3.) A remote terminal (MS1) queries the server (IS). (See id., p. 4, ll. 12-15; Figs. 1-3.) The server (IS) transmits the encrypted location to the remote terminal (MS1) in response to the query. (See id., p. 4, ll. 15-16; Figs. 1-3.) The predetermined encryption key is shared between the mobile device (MS2) and the remote terminal (MS1) but not with the server (IS). (See id., p. 4, ll. 1-3; Figs. 1-3.) The location is decrypted at the remote terminal (MS1) using the predetermined encryption key. (See id., p. 4, ll. 17-19; Figs. 1-2.)

The present invention, as recited in independent claim 2, relates to a mobile device (MS2). The mobile device (MS2) is configured to determine its location. (See id., p. 3, ll. 13-20; Figs. 1-2.) The mobile device (MS2) is further configured to encrypt its location using an encryption key. (See id., p. 4, ll. 4-8; Figs. 1-2.) The mobile device (MS2) is further configured to transmit the encrypted location to a server (IS). (See id., p. 3, ll. 26-30; Figs. 1-3.) The mobile device (MS2) is further configured to share the predetermined encryption key with a remote terminal (MS1) but not the server (IS). (See id., p. 4, ll. 1-3; Figs. 1-3.)

The present invention, as recited in independent claim 3, relates to a server (IS). The server (IS) is configured to receive and store an encrypted location which is encrypted with an encryption key and which corresponds to a mobile device (MS2). (See id., p. 3, ll. 26-30; p. 4, ll. 4-8; Figs. 1-3.) The server (IS) is further configured to transmit the encrypted location to a remote terminal (MS1) in response to a query from the remote terminal (MS1). (See id., p. 4, ll. 12-16; Figs. 1-3.) Between receipt and transmission of the encrypted location by the server (IS), the server (IS) is not in possession of the encryption key. (See id., p. 4, ll. 1-3, 22-23; Figs. 1, 3.)

The present invention, as recited in independent claim 4, relates to a terminal (MS1). The terminal (MS1) is configured to query a remote server (IS) for the location of a particular mobile device (MS2) with which it has shared an encryption key independently of the server (IS). (See id., p. 4, ll. 1-3, 12-15; Figs. 1-3.) Upon receipt of an encrypted location encrypted with the encryption key, the terminal (MS1) is further configured to decrypt the location. (See id., p. 4, ll. 17-19; Figs. 1-2.)

6. Ground of Rejection to be Reviewed on Appeal

I. Whether claims 1-4 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent 7,013,391 to Herle et al. (hereinafter "Herle").

7. Argument

I. The Rejection of Claims 1-4 Under 35 U.S.C. § 103(a) Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 1-4 under 35 U.S.C. § 103(a) as unpatentable over Herle. (See 2/22/08 Office Action, pp. 3-6.) In the Advisory Action, the Examiner restated the grounds for rejection provided in the Final Office Action. (See 6/12/08 Advisory Action, p. 2, line 11.)

Herle includes a mobile station location server that determines a mobile station's location through various locating techniques or by receiving the location information from the mobile station over an encrypted channel. The server stores the location in memory that may be accessed by authorized client access devices. A requesting client access device transmits a request to the server. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit the information in either an encrypted or decrypted form to the device. (See Herle, Abstract.) The server also holds within its memory profile fields of the mobile stations, authorized client profile fields, and encryption-decryption keys. (See id., col. 5, ll. 55-57.) Using the different fields and keys, the server authenticates and transmits the location information. (See id., col. 5, l. 59 – col. 6, l. 8.)

B. Herle Does Not Disclose Sharing the Predetermined Encryption Key Between the Mobile Device and the Remote Terminal But Not With the Server As Recited in Claim 1.

Claim 1 recites "sharing the predetermined encryption key between the mobile device and the remote terminal but not with the server." The Examiner admits that Herle "does not explicitly refer to **not sharing the encryption key with the server**." (See Office Action 2/22/08, p. 4) (emphasis in original). However, the Examiner asserts that Herle's disclosure that "*MS position server application program 330* ***may*** *also be responsible for controlling access to mobile station database 360*" and "an embodiment in which the server **transmits the encrypted position data to the client device which encrypts the position data**" renders the above recited limitation obvious. (See Id.) (emphasis in original). Applicant respectfully disagrees. The entirety of Herle neither teaches nor suggests the above recited limitation.

Specifically, Herle states that, "Wireless mobile stations will soon be required to be able to determine their geographic location. This location information is required to be relayed **only to the wireless service provider or a Public Service Access Point**...While this position is necessary for emergency purposes, it would also be useful for targeting commercial services." (See Herle col. 1, ll. 17-32). Herle further states that, "The present invention encompasses an apparatus for transferring geographic location information associated with the mobile station to a **server** accessible via a communication network coupled to the wireless network. The apparatus comprises memory that stores mobile station current position information **and at least one encryption/decryption key**." (See Herle col. 1, ll. 45-50). Thus, the entire purpose of Herle is to share the encryption key with the server. This clearly is not a suggestion to **not** share the encryption key with the server.

Turning to the specific embodiments pointed out by the Examiner. First, the Examiner asserts that "MS position server application program may also be responsible for controlling access to mobile station database 360" suggests not sharing the encryption key with the server. (*See* Office Action 2/22/2008 p. 4). However, Herle, within the same paragraph, states that "[f]or example, if a request is received for location information for a particular mobile station, that request **must contain a proper decryption key**. MS position server application program determines if that decryption key is accurate so that the requesting entity can access the location information." (See Herle, col. 6, ll. 3-8). That is, Herle states that the server determines if the decryption key is accurate before allowing the requesting entity to access the location information. This clearly is not equivalent to "sharing the predetermined encryption key between the mobile device and the remote terminal but **not with the server**." Furthermore, there is nothing in this embodiment which suggests not sharing the encryption key with the server. The Examiner simply takes a single statement out of context of the described embodiment. Neither the statement itself nor the embodiment is suggestive of the claim limitation.

Herle goes on to further contradict the Examiner's assertion that at the time of the invention one of ordinary skill would have made an embodiment that prevented the server from having access to the encryption/decryption key. Herle specifically states that the server "contains … encryption-decryption key(s) 363." (See Herle col. 5, ll 55-57). Furthermore, Herle states that when a request is made the server will "authenticate the client access … if the client access device properly authenticates … server transmits the encrypted MS 111 position data" or "MS location server 160 decrypts the MS 111 position data and transmits unencrypted MS 111 position data to authenticated client device." (See Herle col. 6, ll. 48-60). In all embodiments, the server stores the encryption/decryption key so that it is able to decrypt the position.

In the Advisory Action, the Examiner specifically relied on the embodiment disclosed on col. 6, ll. 52-56 of Herle to teach this limitation. (See Advisory Action, 6/12/08, p. 2, line 11). Applicant respectfully disagrees with the Examiner's characterization of Herle's teaching. The cited portion of Herle relied on by the examiner states that when the client access device properly authenticates, the MS location server transmits the encrypted position data to the client access device. (See Herle col. 6 ll. 52-56). In this embodiment, the client access device requests authentication from the server, for which the server verifies the user name and password. (See Herle col. 6 ll. 50-52). If the authentication is accepted, the server then transmits encrypted position data to the client access device. (See Herle col. 6 ll. 50-52). Neither this embodiment nor any other embodiment of Herle teaches or suggests "sharing a predetermined encryption key between a mobile device and a remote terminal **but not with the server**" as recited in claim 1.

Additionally, the Examiner in responding to similar previous arguments stated that "the applicant . . . should understand that the statement previously quoted does not exclude from the invention the embodiment described by Herle in which the mobile station shares its encryption key with the remote mobile station only." (See Office Action 2/22/2008 p. 2). Applicant respectfully disagrees with the Examiner's characterization of Herle's teaching. The cited portion of Herle relied on by the Examiner states that the mobile station gives out its location only to those having authorization from the mobile station user. However, all the embodiments of Herle teach that the interface for all the mobile stations is the server to obtain this information and the server has the encryption key.

There is no embodiment described or suggested in Herle where the encryption key is not shared with the server. Therefore, Applicant submits that claim 1 is patentable over Herle.

C. Herle Does Not Disclose a Mobile Device Configured To Share the Predetermined Encryption Key With a Remote Terminal but Not the Server As Recited in Claim 2.

Claim 2 recites "[a] mobile device configured to ... and share the predetermined encryption key with a remote terminal but not the server." Appellant respectfully submits that Herle does not disclose "shar[ing] the predetermined encryption key with a remote terminal but not the server" for the reasons stated above with reference to claim 1. Accordingly, the rejection of claim 2 over Herle should be overturned.

D. Herle Does Not Disclose Wherein Between Receipt and Transmission of The Encrypted Location By the Server, the Server Is Not In Possession of The Encryption Key As Recited in Claim 3.

Claim 3 recites "[a] server configured to receive and store an encrypted location which is encrypted with an encryption key... wherein between receipt and transmission of the encrypted location by the server, the server is not in possession of the encryption key." Appellant respectfully submits that Herle does not disclose a server that "is not in possession of the encryption key" for the reasons stated above with reference to claim 1. Accordingly, the rejection of claim 3 over Herle should be overturned.

E. Herle Does Not Disclose A Terminal Configured To Query a Remote Server For the Location of a Particular Mobile Device With Which It Has Shared an Encryption Key Independently of the Server As Recited in Claim 4.

Claim 4 recites "A terminal configured to query a remote server for the location of a particular mobile device with which it has shared an encryption key independently of the server..." Appellant respectfully submits that Herle does not disclose "shar[ing] an encryption key independently of the server" for the reasons stated above with reference to claim 1. Accordingly, the rejection of claim 4 over Herle should be overturned.

8. Conclusion

For the reasons set forth above, Appellant respectfully requests that the Board reverse the rejection of the claims by the Examiner under 35 U.S.C. § 103(a), and indicate that claims 1-4 are allowable.

Respectfully submitted,

Date: August 19, 2008

By: ______________________
Michael J. Marcin (Reg. No. 48,198)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel.: (212) 619-6000
Fax: (212) 619-0276

CLAIMS APPENDIX

1. (Previously Presented) A method of distributing the location of a mobile device comprising the steps of:

determining the location of the mobile device

encrypting the determined location using an encryption key;

transmitting the encrypted location to a server;

storing the encrypted location at the server;

querying the server from a remote terminal;

transmitting from the server to the remote terminal the encrypted location in response to the query;

sharing the predetermined encryption key between the mobile device and the remote terminal but not with the server; and

decrypting the location at the remote terminal using the predetermined encryption key.

2. (Previously Presented) A mobile device configured to determine its location, encrypt its location using an encryption key, transmit the encrypted location to a server, and share the predetermined encryption key with a remote terminal but not the server.

3. (Previously Presented) A server configured to receive and store an encrypted location which is encrypted with an encryption key and corresponds to a mobile device; and in response to a query from a remote terminal, to transmit to the remote terminal the encrypted location; wherein between receipt and transmission of the encrypted location by the server, the server is not in possession of the encryption key.

4. (Previously Presented) A terminal configured to query a remote server for the location of a particular mobile device with which it has shared an encryption key independently of the server; and upon receipt of an encrypted location encrypted with the encryption key, decrypting the location.

EVIDENCE APPENDIX

No evidence has been entered or relied upon in the present appeal.

RELATED PROCEEDINGS APPENDIX

No decisions have been rendered regarding the present appeal or any proceedings related thereto.